Should Quantum Key Distribution be Used for Secure Communications?

Summary

Quantum Key Distribution (QKD) presents itself as a technology functionally equivalent to asymmetric key agreement schemes that are used in nearly all secure communication protocols over the Internet or in private networks. The defining characteristic of QKD is its alleged superior secrecy guarantee that would justify its use for high security applications. However, deployment constraints specific to QKD hinder large-scale deployments with high practical security. Furthermore, new threats on existing cryptography, and in particular the emergence of universal quantum computers, are taken into account by upcoming standardized "post-quantum" algorithms.

QKD may find some use in a few niche applications, for instance as a defense-in-depth measure on point-to-point links. However, the use of state-of-the art classical cryptography including post-quantum algorithms is by far the preferred way to ensure long-term protection of data, as it is the only technology choice that offers the functional properties needed in modern communication systems.

In any case, the cost incurred by the use of QKD should not jeopardize the fight against current threats to information systems which overwhelmingly do not exploit cryptographic weaknesses.

For another point of view on this topic with similar arguments and conclusions, the reader may consult the white paper of the National Cyber Security Centre (UK) [1], or the position of the NSA (USA) [2].

What is Quantum Key Distribution?

Quantum Key Distribution is a family of method based on physical principles, unlike classical cryptography which has mathematical foundations, which enables two peers to build a common secret (a key) through a dialogue taking place on public channels. Two channels are required:

- the "quantum channel": a communication channel with properties controlled at the physical level. It is usually an optical fiber or an atmospheric link with direct line of sight; on this channel, for QKD to work, optical losses and noise cannot be too high, but more importantly, *there must be no device interacting with the information exchanged;*
- a regular digital network link, which carries QKD signaling.

As with any method aimed to produce a common secret between two peers, each peer must ensure that it communicates with its intended peer and not with a third party that impersonates it. For this, it is sufficient to authenticate the QKD signaling on the digital network link.

When a QKD system is operational, it produces common secret bits between its endpoints at a variable rate, generally between a few kilobits/sec., and a few megabits/sec.

The capacity of QKD to produce a common secret stems from its ability to detect eavesdropping on the quantum channel using quantum effects (to understand how this works, see for instance an introductory description of some classical QKD protocols including the first one, BB84 [8]), then to bound the amount of information that an eavesdropper may have obtained about the data exchanged on the quantum channel, and to adapt the secret rate accordingly. When an active

device relays data on the quantum channel, the secret rate is zero, because it is indistinguishable from an eavesdropping device. Any device reconstructing the signal on this channel is therefore incompatible with QKD. This includes networking devices (switches, routers, …) and optical amplifiers. *This is why QKD requires direct point-to-point links for the quantum channels.*

The bound on tolerable losses on the quantum channel induces a bound on the maximal distance between endpoints. A 20dB loss limit, which is fairly typical for QKD, corresponds to 100Km of optical fiber in perfect condition with no intermediate connection. Because of poor fiber condition, losses incurred by connections, or suboptimal fiber path, real-world distance at this loss level may be much shorter. Larger distances may be crossed using satellite QKD links, which require dedicated hardware in space.

What are the uses of QKD?

QKD is usually promoted as a means to build secure communications, i.e. communications that ensure message confidentiality and integrity.

Secure communications are massively used today; they are built in any web browser communicating over the Internet, they enable to connect physically separate corporate networks, or mobile devices to private networks. Inside networks, they are used to protect machine-to-machine or service-to-service communications.

Secure communications are created in a two-step process: in a first step, a key agreement uses an *asymmetric* cryptographic mechanism (based today on RSA or a variant of the Diffie-Hellman scheme) to authenticate peers and build a common secret between them; in a second step, this common secret or *key* is used to ensure message confidentiality and integrity through *symmetric* cryptography mechanisms (for instance based on the standardized algorithm AES).

QKD can replace the use of asymmetric key agreement schemes to produce the common key, which is then used in symmetric schemes to protect messages. In this scenario, the secret key rate of QKD does not limit the data rate of secure communications, since a short key (typically 128 or 256 bits) enables the protection of large volume of messages. However, this combination still depends on computational cryptographic mechanisms (i.e. mechanisms whose security depends in principle on the computing power of an adversary, or its expertise in cryptanalysis).

QKD can also be used without symmetric cryptography to provide communication security independently of an adversary's computational power. In that case, message confidentiality is provided by the one-time-pad encryption scheme which uses one bit of key to protect each bit of message. Similarly, message integrity can be provided by schemes that are immune to computational attacks. In that scenario, the data rate is limited by the key rate of QKD, typically to values between 1,000 and 1,000,000 times lower than what can be obtained with symmetric schemes. The very low resulting data rate is unsuitable for most applications.

Finally, QKD is sometimes described as being able to protect data at rest. This is a misnomer: in fact, data is encrypted using means unrelated to QKD and a key, then this key is transported to some storage space distinct from the data storage space, possibly after having been split in several parts with the help of a secret sharing scheme. It is therefore more an application of QKD-assisted secure communications, than a distinct QKD functionality.

Are there new services provided by QKD? Where can it be used?

As seen in the previous paragraph, *all services provided by QKD can also be provided by existing technologies.* Setting aside for a moment its security properties, the right question about QKD use-

cases is therefore: what subset of current uses of secure communications can reasonably be provided by QKD, in light of its practical limitations?

Beyond limitations related to the quantum channel (range, incompatibility with active devices), the mere fact that QKD requires specific hardware puts it at a distinct disadvantage in all cases where cryptography is implemented in software. This prevents it from providing end-to-end security for instance between virtualized environments or between software services.

The most reasonable use for QKD is to provide, together with symmetric encryption, communication security between fixed locations that are sufficiently close to each other and connected by an optical fiber.

What threats does QKD protect against? Does it have any weakness?

The main advantage of QKD is to be immune to computational attacks aimed at recovering the secrets produced. In current key negotiation schemes using asymmetric cryptography, an adversary looking to obtain the negotiated secret has all the information it needs to do so, but must solve some mathematical problem to succeed. The resolution of this problem with the best methods known today requires an amount of computation that is completely unrealistic, even with optimistic estimates of the increase of the available computing power in the next decades. However, there is no *proof* that current methods cannot be improved significantly; better techniques may make this problem solving feasible. To put it differently, there is no proof that current key negotiation schemes are robust against any adversary with unknown capacities or knowledge.

This problem, which is an old one in the history of computer science and mathematical cryptography, has taken a new turn with current research about *universal quantum computers*. It is indeed proven that such a machine, if it were to be built, would solve much more efficiently than current computers the mathematical problems associated with asymmetric key negotiation methods used today (factorization of large integers for RSA, discrete logarithm problem for Diffie-Hellman), to the point of making these methods totally insecure. It is not expected however that the existence of a universal quantum computer would threaten significantly the security of symmetric cryptography. This is what motivates the discourse legitimizing the switch from asymmetric key negotiation to QKD; all the more so if one is concerned about the long-term security of data exchanged today, which requires dealing with the threat of quantum computers *before* it becomes a reality, since exchanged data can be stored for later cryptanalysis.

As we shall see, it is perfectly possible to deal with this threat without QKD.

Before that, let us point out that QKD immunity to attacks is not absolute:

- While theoretically QKD protocols are not vulnerable to mathematical attacks, in practice it is very difficult to implement them perfectly. Moreover, an attacker may be able to cause QKD devices to operate abnormally. Deviations from the theoretical protocol, provoked or not, are then likely to compromise security to the point that they lead to practical attacks. This problem, while similar to the problem of side-channels for classical cryptography, is nevertheless specific to QKD and has led to several cryptanalyses of commercial QKD equipment (see for instance [6] for one of the first articles on this topic or [7] for more recent work);

- In addition, QKD devices may have weaknesses unrelated to the quantum protocol used: for example, software vulnerabilities or leakage of secrets by electromagnetic radiation. These issues, which are routinely explored for cryptographic equipment, have seen little scrutiny so far in the case of QKD; a thorough and standardized analysis of QKD products, e.g. following the methodology of Common Criteria [5], is necessary before using it to protect sensitive data. This issue is even more pressing for equipment handling classified data, which must follow strict evaluation procedures aimed at ensuring practical resistance to attacks by nation-state adversaries.

A large-scale QKD deployment creates other security issues.

Can QKD be deployed on a large scale? What level of protection can it provide in such a scenario?

The range limitations of QKD (or the need to use satellites to overcome them), its point-to-point nature, and its dependence on the physical characteristics of the channels it uses, make its large-scale deployment extremely complex and costly. More importantly, in the absence of a direct line connecting two points which need to negotiate a common key, users are led to negotiate keys in sections along a path composed of several QKD links, *which requires trust in the intermediate nodes of the communication (which are called for this reason trusted nodes) and is a major regression compared to current end-to-end key negotiation methods*. The alternative of directly linking all nodes that need to communicate is not feasible in practice except for small networks, both in terms of the number of terminations and geographical extension. In the future, trusted nodes may be superseded by “quantum repeaters” which will not have to be trusted; but this technology has not been demonstrated to work in a lab, let alone in the field.

While the use of satellites extends the range of QKD, it does not generally allow end-to-end information protection unless both ends of the communication have their own satellite ground infrastructure; it is also based on the assumption that each satellite is itself a trusted node, which implies that the risk of computer intrusion in satellites is completely eliminated.

Classified networks constitute a particular challenge to QKD. Indeed, keys used to protect classified communications should be obtained from QKD equipment sitting in the classified network itself. Unlike regular encryptors, different QKD devices cannot easily share the same communication link for their quantum channel; therefore, the only straightforward way to deploy QKD in a classified network is to use a QKD infrastructure *specific to that network.* With several networks of different classification levels, this leads to extremely costly infrastructure duplication, or to the use of the same QKD equipment for different classification levels which is in general not permitted by regulations applying to classified networks.

Beside QKD, what are the alternatives to current key negotiation mechanisms?

The threat of quantum computers has been considered by the cryptographic community for many years. New “quantum-safe” asymmetric algorithms are being standardized (mainly through the competition organized by the NIST [3]) to replace those vulnerable to quantum computing. Candidates are already available today, and over the next decade, significant efforts will be devoted to their deployment in secure communications software products and libraries. In contrast to the use of QKD, this deployment will not require any significant functional alteration of the services using these algorithms.

As with current asymmetric mechanisms, barring a major theoretical breakthrough, no absolute proof of robustness will be available for these new mechanisms. Rather, the confidence in such mechanisms will be the result of efforts made to uncover their weaknesses and to study the mathematical problems underpinning their security.

The ANSSI recommends an overlap of current and post-quantum algorithms, with a progressive phase-out of the former, as detailed in a separate ANSSI position paper.

Secure networks: technology shootout

The table below presents a summary of the main security and functionality properties of available technologies to build secure networks. Alongside the combination of symmetric and asymmetric cryptography, and QKD paired either with unconditionally secure cryptographic primitives or with computationally secure symmetric encryption, it shows the properties of solutions purely based on symmetric cryptography.

Two main observations can be derived from this: first, PKI-based cryptography is the only choice that has all the functional properties routinely used today: it scales easily including when users change over time and with no need for a unique user management authority; it can provide end-to-end security; its throughput is not limited, and of course, it requires no dedicated infrastructure.

A second, less-known fact is that a purely symmetric-cryptography-based solution compares favorably with practical QKD, that is, QKD paired with symmetric cryptography: it is much easier to deploy than QKD because it only requires standard network infrastructure; and offers comparable security, because it uses the same computational cryptography primitives.

Secure communications based only on symmetric cryptography may by appealing when users sets are fixed or can be managed centrally, and when one sees a value in avoiding the use of asymmetric cryptography altogether, for instance as an extra measure of caution against unknown cryptanalysis algorithms, quantum or otherwise. Publication [4] provides an example of a protocol that could be used in such a case.

References

- [1] White paper – Quantum Security Technologies, NCSC, UK, 2020/03
- [2] Quantum Key Distribution (QKD) and Quantum Cryptography QC, NSA, USA, 2021
- [3] Post-Quantum Cryptography Standardization, NIST, USA
- [4] "Symmetric Authenticated Key-Exchange (SAKE) with Perfect Forward Secrecy", 2019
- [5] Certification critères communs - ANSSI (French)
- [6] "Hacking commercial quantum cryptography systems by tailored bright illumination", 2010
- [7] "Laser seeding attack in quantum key distribution", 2019
- [8] A Survey of the Prominent Quantum Key Distribution Protocols, 2007
- [9] "XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions", 2011

	PKI-based cryptography	**Purely symmetric cryptography**	**QKD with PKI-based signaling**	**Unconditionally secure QKD**
Building blocks	Message encryption and authentication with symmetric cryptography. Keys provided by asymmetric key establishment algorithms authenticated with signatures using a Public Key Infrastructure (PKI).	Message encryption and authentication with symmetric cryptography. Keys initialized offline and possibly managed remotely.	QKD + symmetric cryptography for message encryption and authentication, with QKD keys; QKD signaling authenticated with hash-based signatures using a PKI[1].	QKD paired with unconditionally secure message encryption (i.e. One-Time Pad) and authentication, with QKD keys; QKD signaling authenticated unconditionally, with keys initialized offline and renewed by QKD.
Can be deployed over the Internet or private networks	**Yes**	**Yes**	**No**	**No**
Resists to quantum computers / to cryptanalysis advances	**++**[2]	**+++**[3]	**+++**[4]	**++++** No purely algorithmic attack is possible.
Resists to device/software hacking and side-channel attacks	Not in general. Implementation-dependent.			
Can easily scale and manage users[5]	**Yes**	**No**	**No**[6]	**No**[7]

1 Since hash functions and symmetric encryption algorithms use similar building blocks and security hypotheses, the use of hash-based signatures ensures that the whole scheme only depends on the security of symmetric cryptography.

2 With post-quantum asymmetric algorithms (i.e., algorithms designed to be unaffected by quantum computers) and quantum-resistant symmetric key sizes (256 bits for encryption and 384 bits for hashing when targeting 128-bit security).

3 Assuming quantum-resistant key sizes. Purely symmetric cryptography is widely held to be less prone to cryptanalysis advances than asymmetric cryptography because it has less mathematical structure.

4 Same resistance as when using purely symmetric cryptography, which it is also used here for data encryption and data integrity.

5 User management ease is judged by the capacity to add/remove authorized users dynamically and in a decentralized fashion.

6 Compared to unconditionally secure QKD, QKD signalling key management is easier, but a dedicated infrastructure is nevertheless needed which is the main impediment to scaling. Hash-based signatures may also induce limitations in the volume of QKD signalling traffic that can be authenticated with a given key.

7 Scaling requires adding more hardware and dedicated infrastructure.

Can provide end-to-end security	**Yes**	**Yes**[8]	**No**[9]	**No**[9]
Can achieve high performance (e.g. 100Gb/s encryption)	**Yes**	**Yes**	**Yes**	**No**[10]

8 If the endpoints are specialized devices like link encryptors, the security does not extend to the final user.

9 QKD devices are usually not attached to a unique final user. Trusted nodes also violate end-to-end security.

10 Encryption speed is limited by QKD key rate, typically to a few Kb/s.